CLAIMS

1. A portable data storage device which can interface with a remote computer such as a desktop PC or a portable notebook computer and which is capable of securely storing data in digital format by reference to one or more biometric parameters and wherein such biometric parameters are encrypted by reference to a bioencryption algorithm stored within the device and wherein device is disposed with a biometric sensor, a biometric processing engine, a memory storage facility, a micro-controller, a communications interface, an access decision control unit, a bioparameter storage unit, a combination encryption key generation means, a device code generation means, a data processing unit and a bioencryption engine.

2. A device as claimed in claim 1 wherein the biometric sensor is connected to the biometrics processing engine.

3. A device as claimed in claim 1 wherein the biometric processing engine is connected to an access control decision unit and a bioparameters storage unit.

4 A device as claimed in claim 1 wherein the bioparameters storage unit and the biometric processing engine are further connected with a combination encryption key generation means.

5. A device as claimed in claim 1 wherein the combination encryption key generation means is connected with a device code generation means.

6. A device as claimed in claim 1 wherein the access control unit is connected to the micro-controller and a bioencryption engine.

7. A device as claimed in claim 1 wherein the bioencryption engine is connected to the memory storage means and is reversibly connected with a data processing unit.

8. A device as claimed in claim 1 wherein the data processing unit is connected to the micro-controller.

9. A device as claimed in claim 1 wherein the micro-controller is reversibly connected to the communications interface.

10. A device as claimed in claim 1 wherein the biometric sensor may receive biometric parameters from users and wherein the sensor may be active or passive.

11. A biometric sensor as claimed in claim 10 wherein the sensor may incorporate one or more optical, capacitive, electric field, laser, infra red and or magnetic sensor and wherein the biometric sensor can scan and receive biometric parameters from users.

12. A biometric processing engine as claimed in claim 1 wherein the engine comprises a processor capable of processing digital input from the sensor in accordance with predefined bioprocessing algorithms and wherein such bioprocessed data with encryption can be stored in the memory means.

13. A memory storage means as claimed in claim 1 wherein the storage means may be volatile or non-volatile and wherein the storage means is capable of reversibly receiving and storing data for multi read/write applications.

14. A bioparameters storage unit as claimed in claim 1 wherein bioparameters received from users are stored pending approval of the bioparameters prior to access to the data in the memory storage means.

15. A combination encryption key generation means as claimed in claim 1 wherein the user bio-input key which is generated from the biometrics algorithm based on the user biometric parameter input and a predefined key are combined to generate a new key for encryption of the biodata.

16. A device code generation means as claimed in claim 1 wherein factory preset parameters are stored.

17. An access control decision unit as claimed in claim 1 wherein the access control decision unit evaluates biodata received by the sensor and processed by the biometric processing engine to permit or deny access to the data stored in the memory means.

18. A bioencryption engine as claimed in claim 1 wherein bioparameters from users and factory preset parameters from the device code generator are encrypted and decrypted in accordance with predefined algorithms.

19. A data processing unit as claimed in claim 1 wherein data stored in the memory means is processed prior to access by a user via a

communications interface.

20. A micro-controller as claimed in claim 1 which comprises a processor which incorporates a communications interface whereby a user may interface the data storage device via a host computer.

21. A micro-controller as claimed in claim 20 wherein the micro-controller is disposed with a bioencryption algorithm.

22. A process of encryption of biometric parameters wherein biometric data from users is presented to the biometrics sensor and wherein the biometric sensor reads and transfers the biometric data to the biometric processing engine and wherein the biometric parameter is encrypted by the bioencryption engine by reference to the biometric data and a factory preset parameter in accordance with predefined algorithms in a polynominal process to produce an encryption key and wherein the encrypted biometric data is stored in the memory means.

23. A process of decryption of biometric parameters presented to the biometric sensor by a user wherein the data presented to the biometric sensor is read by the sensor and wherein the said data is then analysed by the access control decision unit in accordance with predefined parameters to ascertain whether the said biodata is in conformity with the enrolled biodata and wherein the bioencryption engine then generates a decryption key in respect of biodata verified by the access control decision unit and wherein the decryption key permits access to the data stored in the memory means.